UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
==========X Indictment: CR-13-607

UNITED STATES OF AMERICA

- against -

PHILLIP A. KENNER, and TOMMY C. CONSTANTINE, also known as "Tommy C. Hormovitis",

Defendants.
==========X

DEFENDANT'S MEMORANDUM OF LAW IN SUPPORT OF RELIEF REQUESTED IN PRETRIAL MOTION

HALEY WEINBLATT & CALCAGNI, LLP
By: Richard D. Haley, Esq. (RH-2011)
Attorney for Defendant, Philip Kenner
1601 Veterans Memorial Highway, Suite 425
Islandia, New York 11749
631-582-5151

PRELIMINARY STATEMENT

This memorandum of law is submitted in support of the defendant's motion to suppress evidence in the form of electronically stored data ("computer files") contained on the hard drive of the defendant's Macbook laptop computer ("Macbook computer") and mobile phone ("I-Phone") seized on November 13, 2013 pursuant to a search warrant. Specifically, the defendant claims that the retention of personal data contained on his Macbook computer and I-Phone by the government for the past fourteen months runs afoul of the Fourth Amendment proscription against unreasonable search and seizures. Under governing law, the remedy for such a constitutional violation is the suppression of evidence contained on the defendant's Macbook computer and I-Phone. Therefore, the instant motion is filed pursuant to subdivision (h) of Rule 41 of the Federal Rules of Criminal Procedure.

Additionally, the defendant seeks to serve subpoenas on several third-party witnesses identified as "John Doe" and "Jane Doe" in the Indictment and two banking institutions pursuant to subdivision (c) of Rule 17 of the Federal Rules of Criminal Procedure. As argued below, compliance with the production of documents as requested in the subpoenas in neither unreasonable or oppressive at this stage of the criminal proceedings inasmuch as trial is currently scheduled to commence on March 23, 2015 and the documents requested in the subpoenas are material and necessary to the defense of the matter.

STATEMENT OF FACTS

On November 13, 2013, the Honorable Bridget S. Bade, United States Magistrate Judge for the District of Arizona, signed a warrant authorizing the seizure of "computers or storage media that contain records or information" regarding a specific category records or information as set forth in

paragraph 1-2 of "Attachment B" to the application for a search warrant, sworn to by special agent Joshua Wayne of the Internal Revenue Service the same day. The warrant authorized the seizure of such records or information from any "COMPUTER" found at 10705 East Cactus Road, Scottsdale, Arizona, the residence of the defendant. Although F.R.Crim.P 41(e)(2)(B) permits the "on-site copying" of computer records, the warrant application requested the physical seizure, rather than on-site "mirror imaging", of any computer hard drive or storage media found on the premises. The definition of "COMPUTER" as set forth on page 4 of the application for search warrant clearly encompasses the seizure of the defendant's Macbook computer and I-Phone.

The rationale for seeking the authorization for off-site review of the electronically stored information contained on the defendant's Macbook computer is found in paragraph 42-a of special agent Wayne's affidavit in which he wrote "(G)iven the ever expanding data storage capabilities of computers and storage media, **reviewing such evidence to identify the items described in the warrant can take weeks or months**, depending on the volume of data stored, and would be impracticable and invasive to attempt on-site" (*emphasis added*). Thus, special agent Wayne recognized that Kenner's Macbook computer and I-Phone likely contained computer files beyond the scope of the records or information described in paragraphs 1-2 of "Attachment B" ("non-responsive computer files") when he applied for the warrant.

Pursuant to the warrant, the defendant's Macbook computer, I-Phone and assorted documents were seized by agents of the Federal Bureau of Investigation on November 13, 2013. On March 24, 2014, the government provided two (2) one-terabyte portable hard drives to defense counsel which were purported to "contain imaged copies of the electronic devices that were recovered from defendant Phillip Kenner's home in Scottsdale Arizona on November 13, 2013."

On July 16, 2014 , defendant requested the return of his "Apple" Macbook computer. In this regard, counsel wrote to the government as follows:

> "Given the technical resources of the Federal Bureau of Investigation, I imagine that the Bureau if fully capable of producing a mirror image of the Macbook computer for its use and has already done so as evidenced by the Rule 16 disclosure and creation of the two hard drives. Indeed, I envision that upon the trial of the matter information contained on the Apple laptop will be presented to the court and jury without its actual use but the use of a mirror hard drive for indexing and display."

The July 16, 2014 proposal for the return of the defendant's Macbook computer was accompanied by an offer of counsel to "execute on behalf of my client a broad based stipulation waiving any and all objections to the admissibility of information contained on the Apple laptop as recreated on the mirror hard drives maintained by the government, subject to objections to relevance, materiality and/or undue prejudice." At a status conference before the Court on September 2,2014, the defendant renewed his request for the return of his Macbook computer, including his I-Phone, and argued that the decision of the Second Circuit in United States v. Ganias required not only the purging of personal information contained on the defendant's electronic devices but also, as a corollary, the return of the defendant's Macbook computer and i-phone, without the need for a "broad based stipulation" which Tommy Constantine, through counsel, declined to execute.

In response to the defendant's request for the return of his Macbook computer and i-Phone, the government argued that, at a bare minium, the defendant's request must await the completion of the "privilege review" by the government's privilege review team before the Court should make any determination of the issue. When the Court inquired "(H)ow much longer is the privilege review process?" the government responded: MR. MISKIEWICZ: "I am advised the should have, if not by

the end of the month certainly by October 15, a list to counsel about what they deem to be privileged or not privileged." Pursuant to the direction of the Court, the instant pre-trial motion is filed to brief the issue since the "privilege review" has now taken place as noted in the following paragraph.

On November 3, 2014, Assistant United States Attorney Catherine M. Mirabile completed the government's "privilege review" and provided under her cover letter "one portable hard drive and four CD's containing copies of the electronic materials seized on November 13, 2013 during the execution of the search warrant at the defendant Phillip Kenner's home in Scottsdale, Arizona." On November 25, 2014, Ms. Mirabile provided replacement CD's with passwords after the computer files on the first set of CD's as well as the portable hard drive could not be accessed because the files were "password protected". At the direction of Ms. Mirabile, the portable hard drive was returned to her and on December 2, 2014 and December 4, 2014 Ms. Mirabile was advised that the computer files contained on replacement CD's, as well as the re-circulated portable hard drive, could not be accessed due to an "error code" screen on the computer which prevented the use of the passwords provided by Ms. Mirabile.

The December 2,2014 letter to Ms. Mirabile advised her that the officials at the Queens Private Correctional Center, where the defendant is incarcerated, will not allow CD's containing computer files to be provided to an inmate if the content of the CD's cannot be viewed by such officials prior to release to the inmate. In this regard, telephone number of the defendant's counselor at the Queens Private Correctional Center was provided to Ms. Mirabile to verify that he encountered the same "error code" message preventing the use of the passwords to open the computer files. As of the date of this memorandum of law, no further communication has been received from Ms. Mirabile.

As set forth in the accompanying affidavit of the defendant in support of the instant motion, the non-responsive computer files contained on his Macbook computer are easily identifiable. Similarly, the defendant's i-Phone contains a vast quantity of personal information–a fact of modern day life recently recognized by the Supreme Court in Riley v. California, 134 S.Ct. 2473, 2488-2491 (2014). The defendant's affidavit also addresses his request for the issuance of subpoenas pursuant to subdivision (c) of Rule 17 of the Federal Rules of Criminal Procedure.

ARGUMENT

A. The Government's Prolonged Retention of Non-Responsive Computer Files Seized During the Execution of a Search Warrant Requires the Suppression of Evidence Consisting of the Responsive Computer Files Seized Pursuant to the Same Search Warrant

In United States v. Ganias, 755 F.3d 125 (2nd Cir. 2014), the Second Circuit addressed a claim by the defendant, Stavos M. Ganias, of a Fourth Amendment violation due to the government's lengthy retention of personal computer files seized pursuant to a warrant by agents of the Army Criminal Investigation Command. There, Army investigators accompanied by computer specialists elected to make "on site" identical copies, or forensic mirror images, of the hard drives of the personal computers belonging Ganias, an accountant for American Boiler and Industrial Property Management ("IPM"), who were under investigation for improper billing and theft of government property. *Id.* at 128-129. On November 19, 2003, the Army investigators created forensic mirror images of Ganias's personal computer files at his office but did not begin to isolate and extract the computer files that were relevant to American Boiler and IPM until July 2004, a process completed in December, 2004. *Id.* at 129. Despite the assurance to Ganias by Army investigator's that personal information unrelated to the current federal investigation as contained on Ganias's computer "would be purged once they completed their search for relevant files", *Id.* at 128, the government

did not purge such information which led to the filing of a suppression motion by Ganias in the District Court for the District of Connecticut on February 27, 2011. On June 24, 2011, the District Court denied the motion which resulted in the continued retention by the government of Ganias's personal computer files and led to the appeal of the District Court's decision to the Second Circuit following Ganias's conviction.

After analyzing Fourth Amendment precedent and reviewing the appellate record, the Court in Ganias wrote "(W)e conclude that the Government violated Ganias's Fourth Amendment rights by seizing and indefinitely retaining non-responsive computer records." *Id.* at 141. In support of its conclusion, the Court noted that the Fourth Amendment was enacted primarily to protect the public against "general warrants" used by the British Crown, a practice "(T)he Framers abhorred, believing that 'papers are often the dearest property a man can have' and that permitting the Government to 'sweep away all papers whatsoever without any legal justification would destroy all the comforts of society.'" *Id.* at 134 (citation omitted); *see also* Riley, *supra*, 134 S.Ct. at 2494. Because the Fourth Amendment requires that the warrant state with particularity the areas to be searched and the items to be seized, *citing* United States v. Galpin, 720 F.3d 436, 445 (2nd Cir. 2013), the Court wrote that "(T)his restricts the Government's ability to remove all of an individual's papers for later examination because it is generally unconstitutional to seize any item not described in the warrant" (*citations omitted*). The Court then held that "(T)hese Fourth Amendment protections apply to modern computer files..." *Id.* at 139.

In the instant case, the government elected to physically seize the defendant's Macbook computer and i-Phone, which contained personal computerized files and information outside the scope of the warrant, instead of an "on-site coping of the media or information consistent with the

warrant" as authorized by F.R.Crim.P 41(e)(2)(B) ("Rule 41"). In so doing, the government immediately deprived the defendant of access to computer files containing personal financial records, personal correspondence, intimate videos and pictures, family pictures, music, personal internet downloads and other items of a personal nature. Although Rule 41 does not require the government to conduct on-site copying or on-site forensic analysis of computer files, the holding in Ganias does require that the Government purge "non-responsive computer records" within a reasonable period of time. Here, the government seized the defendant's computer records on November 13, 2013, which contained computer files arguably responsive to the items particularized in the warrant ("responsive computer files") as well as highly personal computer files ("non-responsive computer files"), yet has retained non-responsive computer files belonging to the defendant for the past fourteen months and continues to do so through the retention of the defendant's Macbook computer and i-Phone. Under the authority of Ganias, the prolonged retention of the defendant's personal computer files requires the suppression evidence in the form of electronically stored data contained on the hard drive of the defendant's Macbook computer and i-Phone seized on November 13, 2013.

The fact that the government was constitutionally required to conduct a "privilege review" before releasing the responsive computer files to the prosecution team and its investigators does not remedy the Fourth Amendment violation established in Ganias. As part of the privilege review team, Ms. Mirabile and the federal agents working with her are government employees who have a constitutional obligation to purge non-responsive computer files in their possession. Presumably, the privilege review team obtained a mirror image of the computer files shortly after the seizure of the defendant's Macbook computer and i-Phone on November 13, 2013 in order to conduct its

"privilege review" but certainly possessed a mirror image of the computer files on March 24, 2014 when two (2) one-terabyte portable hard drives to defense counsel which were purported to "contain imaged copies of the electronic devices that were recovered from defendant Phillip Kenner's home in Scottsdale Arizona on November 13, 2013." On November 3, 2014, Ms. Mirabile possessed "one portable hard drive and four CD's containing copies of the electronic materials seized on November 13, 2013 during the execution of the search warrant at the defendant Phillip Kenner's home in Scottsdale, Arizona" which were provided to counsel. Ostensibly, Ms. Mirabile possessed the same set of identical copies of the computer files for her on use long before additional computer generate copies were provided to the defendant.

It is recognized that a Fourth Amendment violation may not result in the suppression of evidence when there is a widespread seizure of items not covered by the warrant if the law enforcement agents act in good faith. Ganias, 755 F.3d at 140, *citing* United States v. Shi Yan Liu, 239 F.3d 138 (2nd Cir. 2000). After observing that "(I) is the Government's burden...to demonstrate the objective reasonableness of the officer's good faith", the Court found that established Fourth Amendment precedent precluded the government from relying upon the good faith defense. Here, of course, the government has yet to purge the non-responsive computer files on the mirror imaged copies even though the Second Circuit rendered its decision in Ganias on June 17, 2014 and the defendant cited the Ganias precedent in his argument before the Court on September 2, 2014. Thus, the good faith defense in this case is even less availing inasmuch as the retention of non-responsive computer files belonging to the defendant continues to this date due to the retention of the defendant's Macbook computer and i-Phone.

Finally, the government's reason in the instant case for retaining the non-responsive computer

files contained on the defendants Macbook computer and i-Phone was addressed by the Court in Ganias. There, the government argued that "...returning or destroying the non-responsive files is entirely impractical because doing so would compromise the remaining data that was responsive to the warrant, making it impossible to authenticate or use it in a criminal prosecution." *Id.* at 139. In response, the Court wrote that "(W)e are not convinced that there is no other way to preserve the evidentiary chain of custody". Indeed, the Army computer specialists in Ganias recognized the authenticity of the "mirror image" computer files and Rule 41 similarly allows such on-site "copying of electronically stored information." Moreover, the Army computer specialists in Ganias did not suggest to Ganias that the "purging" of non-responsive files would compromise the remaining computer files. Simply put, absent credible expert testimony that deletion of the non-responsive computer files will compromise the creation, form or content of the responsive computer file, it is submitted that chain of custody is easily established as long as the responsive "mirror imaged" computer files are secured within the chain of custody by the government agents for introduction as evidence at trial.

B. The Defendant is Entitled to the Issuance of F.R.Crim.P. 17(c) Subpoenas as Necessary and Material to the Defense of the Matter.

In United States v. Tucker, 249 F.R.D 58 (S.D.N.Y 2008), Judge Scheindlin interpreted the provisions of F.R.Crim.P. 17(c) ("Rule 17") in the context of a defendant who requested recordings of telephone calls made by a cooperating witness while incarcerated at a Bureau of Prison's facility. There, the government argued, *inter alia*, that the defendant had not met the standards articulated in United States v. Nixon, 418 U.S. 683 (1984) to warrant the disclosure of the information sought in the proposed Rule 17 subpoena. As noted by Judge Scheindlin, the Nixon standards apply where

the government issues a subpoena or where a defendant issues a subpoena to the government. In the latter event, disclosure is governed by F.R.Crim.P. 16 and, accordingly, disallowed by way of Rule 17 production. Here, of course, Kenner is not seeking disclosure from the government by way of his proposed Rule 17 subpoenas.

Having distinguished Nixon, Judge Schendlin determined that the issuance of a Rule 17 subpoena is appropriate where production of records is requested by "(A) criminal defendant; (B) on the eve of trial; (C) from a non-party; (D) where the defendant has an articulable suspicion that the documents may be material to his defense" *Id.* at 66. Thus, contrary to the Nixon standards, the District Court concluded that "(A) defendant in such a situation need only show that the request is (1) reasonable, construed as 'material to the defense,' and (2) not unduly oppressive for the producing party to respond" *Id.* The rationale for the District Court's decision was premised on "Constitution guarantees" which were rendered "meaningless" if the Rule 17 subpoenas, as modified by the District Court, were quashed. *Id.* at 67.

Here, the information sought in the Rule 17 is tailored to address the allegations set forth in the portions of the Indictment titled "The Scheme to Defraud", "The Hawaii Land Developments", "The Eufora Investments", "The Global Settlement Fund", "The Led Better Fraud Scheme" concerning the "Sag Harbor Property", as well as the "Money Laundering Conspiracy". Moreover, the information sought may serve to impeach the credibility of the third-party witness only insofar as the documentary evidence contradicts his/her testimony. Finally, the Rule 17 subpoenas to be served upon the banking institutions require the production of documents which will reveal knowledge on the part of the defendant's"investment clients", identified as "John Does" 1 through 15 of the Indictment, of the purpose and use of their respective lines of credit, as well as the

defendant's authority to access the lines of credit established by each "John Doe".

CONCLUSION

For the reasons stated above and on the basis of the applicable law, the computerized files contained on the defendant's Macbook computer and i-Phone seized pursuant to a warrant on November 13, 2013 should be suppressed. Additionally, the court should authorize the issuance and service of subpoenas pursuant to F.R.Crim.P 17(c) as requested by the defendant in the accompanying notice of motion and affidavit of the defendant.

Dated: Islandia, New York
January 22, 2015

Richard D. Haley